

1 Jason K. Singleton, State Bar #166170
jason@singletonlawgroup.com
2 Richard E. Grabowski, State Bar #236207
rgrabowski@mckinleyville.net
3 SINGLETON LAW GROUP
611 "L" Street, Suite A
4 Eureka, CA 95501
(707) 441-1177
5 FAX 441-1533

6 Attorneys for Plaintiffs, ASIS INTERNET SERVICES
and JOEL HOUSEHOLTER, dba KNEELAND
7 ENGINEERING, dba FOGGY.NET

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10 ASIS INTERNET SERVICES, a California
11 corporation, and JOEL HOUSEHOLTER, dba
KNEELAND ENGINEERING, dba FOGGY.NET

12 Plaintiff,
13 vs.

14 RICHARD RAUSCH, EDWARD HECKERSON,
15 individually and fictitiously doing business
16 as FIND A QUOTE, and DOES ONE through
FIFTY, inclusive,

17 Defendants.
18

Case No. C-08-3186 EDL

BRIEF IN SUPPORT OF AGGRAVATED
DAMAGES

19 Plaintiff assumes that the Court was referring to **Facebook, Inc. v. Wallace**, Slip Copy,
20 2009 WL 3617789 (N.D.Cal. October 29, 2009) wherein District Judge Fogel grants plaintiff
21 Facebook's request for default judgment and then limits the penalties to \$50 per email and
22 denies treble damages, in the Court's request for brief concerning what penalties should be
23 granted in the matter before the Court.

24 **Penalties are within the discretion of the Court**

25 In **Facebook, Inc. v. Wallace**, Slip Copy, 2009 WL 3617789 (N.D.Cal. October 29,
26 2009) the district court limited the penalties to \$50 per email for 14,214,753 emails per the
27 language of 15 USC § 7706 (g)(3)(A), the same statute is applicable in the within case.
28 Facebook also asked for aggravated damages (treble damages) that would have resulted in an

award of \$4,264,425,900. Judge Fogel further opined that damages for **California Business and Professions Code** §22948.2 at \$1000 per email trebled would amount to \$3,247,500,000.

The district Court held that an award exceeding \$7 billion dollars in a **CAN SPAM Act** action violated the due process rights of the defendant “where the penalty prescribed is so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable.” **United States v. Citrin**, 972 F.2d 1044, 1051 (9th Cir.1992) (quoting **St. Louis, Iron Mt. & S. Ry. Co. v. Williams**, 251 U.S. 63, 66-67, 40 S.Ct. 71, 64 L.Ed. 139 (1919))” **Facebook, Inc. v. Wallace**, Slip Copy, 2009 WL 3617789 at *2 (N.D.Cal. October 29, 2009). Judge Fogel reduced the damages to \$50 per email and declined to apply treble damages for the **CAN SPAM Act** violations. In addition he reduced the **Business and Professions Code** §22948.2 violation to a single incident and a maximum of \$500,000. This still resulted in a default judgment penalty of \$711,237,650. As the court stated “[g]iven the magnitude of this award, the Court declines to award treble damages.” *Ibid*.

In the matter before the Court, **Asis v. Rausch**, many of the detailed facts are similar to those of the **Facebook** case. For example, several other defendants were named in both cases, which the plaintiffs in both cases have dismissed or declined to pursue; leaving only a single defendant that appears to have controlled the efforts of the other defendants. In both cases there was willful disregard of the rights of both the vendors/IAPs and the consumers who were the intended recipients of the emails. In both cases, the emails at issue were egregious violations of the statutes. In both cases, after preliminary appearances the defendants, even after proper notice, refused to appear before the courts. In both cases the courts decided the substantive issues of the case on the basis of information provided by the plaintiffs and the lack of response by the defendants. Procedurally and substantially these cases are very similar with one overriding distinction, the number of violations involved.

The number of emails involved in the **Facebook** case resulted in an award in excess of \$7 billion if aggravated damages were applied. However, in the present matter there are only 24,724 emails at issue and damages are only sought for violations of the **CAN SPAM Act of**

1 **2003.** This consists of: 24,724 emails in violation of 15 USC §7704(a)(1)(A), sending domain
 2 was obtained with a false representation with a penalty of \$100 per email - \$2,472,400; and
 3 24,724 emails in violation of 15 USC §7704(a)(2), misleading or deceptive subject lines, with a
 4 penalty of \$25 per email - \$618,100. As a result total damages of \$3,090,500 trebled for
 5 aggravated damages to \$9,271,500 are requested, plus attorney fees and costs and a
 6 permanent injunction against Defendant Heckerson.

7 ***St. Louis, Iron Mt. & S. Ry. Co. v. Williams***, 251 U.S. 63, 66-67, 40 S.Ct. 71, 64 L.Ed.
 8 139 (1919)) provides the rule for determining if a penalty, that is within the discretion of a court
 9 by way of a statutory penalty, is oppressive. More recently relied on by the 9th Circuit in
 10 ***United States v. Citrin***, 972 F.2d 1044, 1051 (9th Cir.1992). The Supreme Court cautions
 11 that the basis for such judgment cannot be based on a comparison to the actual harm the
 12 violation caused: "When the penalty is contrasted with the overcharge possible in any instance
 13 it of course seems large, but, as we have said, its validity is not to be tested in that way." ***St.***
 14 ***Louis, Iron Mt. & S. Ry. Co. v. Williams***, 251 U.S. 63, 66-67, 40 S.Ct. 71, 64 L.Ed. 139
 15 (1919)). Rather the test proscribed by the Court is whether the penalty is "considered with due
 16 regard for the interests of the public, the numberless opportunities for committing the offense,
 17 and the need for securing uniform adherence". *Ibid*.

18 In this matter it is clearly in the public's interest to stop illegal spamming and that is the
 19 purpose of the statutory penalties. 15 **USC** §7701 et seq. There are obviously numberless
 20 opportunities for committing the offense, in this case Plaintiff has complained of 24,724 non-
 21 compliant emails. Finally, there is a high need to secure compliance. Defendant after initially
 22 appearing has refused to even respond to notices from the Court, much less from Plaintiff.
 23 Defendant has provided nothing but disdain for the Court and the Plaintiff, only through a
 24 significant penalty will compliance be attained. The maximum penalty in this case is
 25 dramatically less than the penalty in the ***Facebook*** case. Even with treble damages the
 26 penalty will be less than \$10 million. Contrasted with the maximum penalty possible in
 27 ***Facebook*** of over \$7 billion, there is little argument possible that the penalty is overly
 28 oppressive or even approaches a violation of due process considered by Judge Fogel.

Therefore the Court should allow the maximum penalty of \$100 per email for each email in violation of 15 **USC** §7704(a)(1) and \$25 per email for each email in violation of 15 **USC** §7704(a)(2) of \$3,090,500. This is the penalty prescribed by the statute and anything less is likely not to have the desired effect.

Aggravated Damages

Aggravated damages are allowed under the **CAN SPAM Act** where either willful intent by the defendant is shown or a violation of 15 **USC** §7704(b) can be demonstrated.

Aggravated damages are allowed under 15 **USC** §7704(b)(1)(A)(i) where evidence of a directory harvest is demonstrated:

“the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages;”

15 **USC** §7706(g)(3)(C).

15 **USC** §7704(b)(2) provides that:

“It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a) of this section.”

Directory Harvest:

This matter contains violations of both sections. A directory harvest can be demonstrated by looking at the actual emails presented in the case. All of the emails contain both the “sent to” email account and the actual “name” of the consumer owning the email account in the header information of the email. Many of these email accounts are closed and have been closed for some time. However, the emails identify the actual consumer who owned the email accounts. The only way anyone could have obtained this information is through a directory harvest of the ASIS email account system. This information does not exist

1 anywhere else and the owners of the accounts no longer have access to the accounts to solicit
2 emails. See Declaration of Nella White ¶¶ 2–6 and Exhibits A and B.

3 In addition, ASIS' web servers contain an Acceptable Use Policy at
4 www.asis.com/aup.html which meets the requirements of 15 **USC** §7706(g)(3)(C). See
5 Declaration of Nella White ¶ 7 and Exhibit C, Acceptable Use Policy.

6 **Use of Automated Scripts:**

7 There were 4,4708 unique email addresses in the “From” headers. The majority of
8 these email addresses followed the pattern name@subdomain. domain.com.

9 The “name” portion of the email address was either related to the product being
10 advertised, for example coloncleanse@ or lowermortgage@, or a common name, like lucy@,
11 jesse@, or joe@. In some instances, newsletter@ was also used.

12 The subdomains used in the “From” headers usually contain a word and a number, for
13 example mail1, mail2, mail3, mail4.

14 The pattern of emails involved sending similar emails from multiple subdomains and
15 domains, using the same “name.” In one instance, Jesse@mx7.grenthe.com,
16 Jess@mx18.greenhe.com, Jesse@mx11.greenhe.com, jesse@m15.oilca.com, and
17 jesse@vmx15.penontatt.com were just a small number of email accounts used in advertising
18 printer ink. See Declaration of Josh Mohland ¶¶ 3–7 and Exhibit A.

19 It is common practice for email spammers to acquire thousands of email accounts and
20 domain names through automated scripts because the current technology identifies the
21 spammer fairly quickly and puts the sending email account, sending domain and the sending
22 IP address on a black list distributed to the filter services/products used by the both the
23 sending ISP and the receiving ISP to block additional further spam emails. See Declaration of
24 Josh Mohland ¶ 8 and Exhibit B.

25 It is clear that these email accounts and domain names were created using an
26 automated script – a program that interacted with web sites that sell domain names and email
27 accounts by filing in the web site and purchasing the accounts using common names from a
28 list, or created names from the product being advertised, or modified the email name or

1 domain name by adding numbers after the name. These scripts acquired thousands of unique
2 email accounts that were then used to send the emails at issue in this matter. For those
3 reasons it is clear that Defendant or Defendant's agents used automated scripts to procure the
4 email accounts and domain names used to send the emails in this matter.

5 **Conclusion**

6 Therefore based on the above arguments and evidence the Court should grant
7 Plaintiff's request for assessment of the maximum penalties allowed under the statute and
8 treble damages.

9
10 **SINGLETON LAW GROUP**

11
12 Dated: April 2, 2010

/s/ Jason K. Singleton

Jason K. Singleton

Richard E. Grabowski, Attorneys for Plaintiffs,

ASIS INTERNET SERVICES and JOEL

HOUSEHOLTER, dba KNEELAND

ENGINEERING, dba FOGGY.NET